UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/763,601 | 01/23/2004 | Daniel Bleichenbacher | 5 | 7709 |

46303 7590 09/04/2008

RYAN, MASON & LEWIS, LLP
1300 POST ROAD, SUITE 205
FAIRFIELD, CT 96824

| EXAMINER | |
|---|---|
| BESROUR, SAOUSSEN | |
| ART UNIT | PAPER NUMBER |
| 2131 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 09/04/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/763,601 | BLEICHENBACHER, DANIEL | |
| | Examiner | Art Unit | |
| | SAOUSSEN BESROUR | 2131 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *20 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/25/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This action is in response to the communication filed 5/20/2008.

2. Claims 1-16 were received for consideration.

3. Claims 1-16 are pending.

### *Election/Restrictions*

4. In view of applicant's arguments, Restriction has been withdrawn.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. **Claims 1-16** are rejected under 35 U.S.C. 102(b) as being anticipated by Takaragi et al. (6,141,421).

As per **claim 1 and 13**, Takaragi discloses: generating a compressed Rabin signature based on a continued fraction expansion of s/n (Column 14, lines 21-32 Column 15, Lines 9-15).

As per **claim 8 and 15**, Takaragi discloses: applying a message formatting function, h, to the message, m, to computing h(m) (Column 10, Lines 27-50); computing a value, t, as h(m)v2 mod n (Column 10, Lines 50-65, Column 14, Lines 32-57); obtaining a value, w, as a square root of the value, t (Column 11, Lines 1-24);

computing a signature value, s, as w/v mod n; and providing a decompressed signature (s,m) (Column 11, Lines 1-24).

As per **claim 10**, Takaragi discloses: computing principal convergent, ui/vi, of a continued fraction expansion of s/n (Fig. 3-4, Column 8, Lines 3-5); establishing an index *l*, such that v/ <n^(1-1/e) <= v/+1 (Fig. 3 Column 8, Lines 6-20); and generating a compressed Rabin signature (vt, m) (Fig. 3 Column 8, Lines 21-28).

As per **claim 11**, Takaragi discloses: applying a message formatting function, h, to the message, m, to computing h(m) (Column 10, Lines 27-50); computing a value, t, as h(m)v^e mod n (Column 10, Lines 50-65, Column 14, Lines 32-57); determining whether the values t or t-n have an eth root over integer values (Column 11, Lines 1-24); computing a value, w, as the eth root; and computing the decompressed signature (w/v mod n, m) (Column 11, Lines 1-24).

As per **claim 2 and 14**, rejected as applied to claim 1. Takaragi discloses: computing principal convergents, Ui/Vi, for i equal to 1 to k, of a continued fraction expansion of s/n, where k is a largest integer for which principal convergents are defined (Fig. 3-4, Column 8, Lines 3-5); establishing an index l, such that vl ~n v/+1 (Fig. 3 Column 8, Lines 6-20); and
generating a compressed Rabin signature (vt, m) for a message, m (Fig. 3 Column 8, Lines 21-28).

As per **claim 3**, Takaragi discloses: computing principal convergent, ui/vi, of a continued fraction expansion of s/n (Fig. 3-4, Column 8, Lines 3-5); establishing an

index /, such that v/ <square root n <= v/+1 (Fig. 3 Column 8, Lines 6-20); and generating a compressed Rabin signature (vt, m) (Fig. 3 Column 8, Lines 21-28).

As per **claim 4**, rejected as applied to claim 3. Takaragi discloses: wherein sv=u(mod n) (Column 8, lines 11).

As per **claim 5**, rejected as applied to claim 3. Takaragi discloses: wherein Ivl<= square root (n) (Column 8, Lines 6-20).

As per **claim 6**, rejected as applied to claim 3. Takaragi discloses: wherein Iul<= square root (n) (Column 8, Lines 6-20).

As per **claim 7**, rejected as applied to claim 1. Takaragi discloses: wherein said principal convergents, ui/vi, are computer for i equal to 1 to k, where k is a largest integer for which principal convergents are defined (Fig. 3-4, Column 8, Lines 3-5).

As per **claim 9, 12 and 16**, rejected as applied to claim 8, 11 and 15. Takaragi discloses: comprising the step of generating an error if no integer square root exists, because it is obvious since decimal numbers are not excepted by the algorithm.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SAOUSSEN BESROUR whose telephone number is (571)272-6547. The examiner can normally be reached on M-F 8:30am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. B./
Examiner, Art Unit 2131
August 27, 2008
/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131